Spoonbill

spoonbill.dev · hello@spoonbill.dev

Security and privacy

Updated October 16, 2026

For IT, security and records review

Spoonbill answers planning questions from a city's own published documents: its code, fee schedules, plans and parcel records. A city uploads nothing to start; the documents are public records it has already published. This page sets out how we handle the data your staff create.

WHERE YOUR DATA LIVES

- Your accounts, conversations and document index are stored in the United States.
- Accounts and conversations: **Cloudflare**. The search index of your city's documents: **Pinecone**, on Amazon Web Services (US East). Document automation: **Railway**.
- AI processing: **Anthropic** and **Google**. Google's terms allow it to process a request briefly outside the United States.

WHAT WE HOLD ABOUT YOUR STAFF

- **Accounts:** name, work email, city, last sign-in.
- **Conversations:** the questions asked and the answers, with their sources.
- **Sign-in records:** a fingerprint (hash) of each sign-in link, never the link, and session records with the browser type.
- No Social Security numbers, financial or health information. Nothing in the product needs residents' personal information.

SIGN-IN AND ACCESS

- **No passwords.** Staff sign in with a single-use link sent to their work email.
- A requested link lasts 24 hours; an invitation link, 7 days. Each works once.
- Sessions last 60 days, in a cookie marked HttpOnly, Secure and SameSite.
- Each person sees only their own conversations, and every account belongs to one city.

ENCRYPTION

- In transit: HTTPS (TLS) on every connection.
- At rest: the databases and the document index are encrypted by their platforms (AES-256).

AI AND YOUR DATA

- Answers are written only from passages retrieved from your city's own published documents and the conversation in progress, never from the open web, and every answer cites its source.
- **No provider may train on what we send:** Anthropic's commercial terms forbid it, Google's paid service does not use prompts or responses to improve its products, and Pinecone's terms grant no such right.
- We never sell data.

RETENTION AND RECORDS REQUESTS

- Conversations are kept while the account is open and for one year after it closes.
- Used or expired sign-in links and sessions are deleted after 30 days.
- Staff cannot delete conversations, because their questions may be public records under your schedule. We export a city's conversations on request; we do not answer a records request on the city's behalf.

BACKUPS AND INCIDENTS

- The account database can be restored to any minute within the last 30 days.
- If we confirm a security incident affecting your data, we notify your named contact by email and phone within 72 hours, and send a written summary within 7 days: what happened, what was affected, what we did and what we are changing.

ACCESSIBILITY AND PAPERWORK

- Built to WCAG 2.1 AA and Section 508. Accessibility Conformance Report (VPAT): spoonbill.dev/vpat-2026-10.pdf.
- On request at hello@spoonbill.dev: a data processing agreement, a W-9 and answers to your security questionnaire.